Examen final de Álgebra II

Miércoles, 16 de junio de 2004

SOLUCIONES

Solución del problema 1. (a) R es un ideal en $\mathbb{Z}_{10}$, $R = \langle 2\rangle \subset \mathbb{Z}_{10}$, en particular un subanillo conmutativo. Lo único que falta para comprobar que es cuerpo es que existen elemento neutro e inverso de la multiplicación. El elemento neutro es 6 porque módulo 10 se tiene:

$$0\cdot 6 = 0, \quad 2\cdot 6 = 2, \quad 4\cdot 6 = 4, \quad 6\cdot 6 = 6, \quad 8\cdot 6 = 8.$$

Y todos los elementos no nulos poseen inverso porque módulo 10

$$2\cdot 8 = 8\cdot 2 = 6, \quad 4\cdot 4 = 6, \quad 6\cdot 6 = 6.$$

(b) La característica es 5 porque $6,\ 6+6,\ 6+6+6,\ 6+6+6+6$, son no nulos y $6+6+6+6+6 = 0$, siempre módulo 10.

(c) $\mathbb{F}_5$, gracias al isomorfismo $\phi : R \longrightarrow \mathbb{F}_5$ dado por reducir módulo 5. Evidentemente ϕ está bien definida y es homomorfismo, $\phi(x\cdot y) = \phi(x)\phi(y)$, $\phi(x+y) = \phi(x)+\phi(y)$ y $\phi(6) = \overline{1}$. Además ϕ es inyectiva, $\mathrm{Ker}\phi = \{0\}$, y por tanto el cardinal de su imagen es $5 = |\mathbb{F}_5|$, por lo que es biyectiva.

Errores más comunes. (b) Según la definición de característica hay que sumar consigo mismo el elemento neutro de la multiplicación.

(c) Que dos grupos sean isomorfos no implica que al dotarlos de estructura de anillo lo sean. Por ejemplo, $\mathbb{F}_{25}$ y $\mathbb{Z}_5 \times \mathbb{Z}_5$ tienen grupos aditivos isomorfos (y por tanto los mismo órdenes de elementos) y sin embargo no son anillos isomorfos: el primero es un cuerpo y el segundo no.

Solución del problema 2.

(a) $\sqrt[5]{2} + 5\sqrt[5]{4} = \sqrt[5]{2} + 5(\sqrt[5]{2})^2 \in \mathbb{Q}(\sqrt[5]{2})$ por tanto la extensión del enunciado es una subextensión de $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ y se debe tener:

$$5 = [\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}(\sqrt[5]{2} + 5\sqrt[5]{4})][\mathbb{Q}(\sqrt[5]{2} + 5\sqrt[5]{4}) : \mathbb{Q}]$$

(la primera igualdad porque $x^5 - 2$ es el polinomio mínimo de $\sqrt[5]{2}$). Por consiguiente el grado pedido es 1 ó 5. Y no puede ser 1 ya que en ese caso $\sqrt[5]{2} + 5\sqrt[5]{4} = r \in \mathbb{Q}$, lo cual es una contradicción, por ejemplo porque entonces $P = x + 5x^2 - r$ se anularía en $\sqrt[5]{2}$ y tendría grado menor que el polinomio mínimo.

(b) Como $\sqrt{3} = (\sqrt[4]{3})^2$, se cumple

$$\mathbb{Q}(\sqrt{3} + \sqrt{-3}, \sqrt[4]{3}) = \mathbb{Q}(\sqrt{3} + i\sqrt{3}, \sqrt[4]{3}) = \mathbb{Q}(i\sqrt{3}, \sqrt[4]{3}) = \mathbb{Q}(i, \sqrt[4]{3}).$$

El polinomio $x^2 + 1$ es el mínimo de i sobre $\mathbb{Q}(\sqrt[4]{3})$ porque si no fuera irreducible se tendría $i \in \mathbb{Q}(\sqrt[4]{3})$ lo cual es contradictorio (el último cuerpo es real). Así pues el grado pedido es dos.

(c) Sea $\zeta = e^{2\pi i/31}$. Sabemos que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 30$ porque el polinomio mínimo de ζ es el polinomio ciclotómico $x^{30} + x^{29} + \cdots + x + 1$. Por la fórmula de Euler, $\cos(2\pi/31) = (\zeta + \zeta^{-1})/2$. Operando, ζ es raíz del polinomio $x^2 - 2x\cos(2\pi/31) + 1$. De aquí, $\mathbb{Q}(\zeta)/\mathbb{Q}(\cos(2\pi/31))$ es una extensión de grado a lo más dos, y no puede ser uno porque $\zeta \notin \mathbb{Q}(\cos(2\pi/31))$, ya que ζ no es un número real. En definitiva:

$$30 = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\cos(2\pi/31))] \cdot [\mathbb{Q}(\cos(2\pi/31)) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\cos(2\pi/31)) : \mathbb{Q}]$$

y el grado de $\mathbb{Q}(\cos(2\pi/31))/\mathbb{Q}$ es 15.

(d) Sabemos que si P es irreducible, $K[x]/\langle P\rangle$ es isomorfo a $K(\alpha)$ donde α es una ráiz de P en su cuerpo de descomposición. En particular el grado requerido es el mismo que el de $\mathbb{F}_2(\alpha)/\mathbb{F}_2$ donde α es raíz de $x^2 + x + 1$, que es su polinomio mínimo sobre $\mathbb{F}_2$ (ya que es mónico e irreducible: $0^2 + 0 + 1, 1^2 + 1 + 1 \neq 0$). Por consiguiente $[L : \mathbb{F}_2] = [\mathbb{F}_2(\alpha) : \mathbb{F}_2] = \partial(x^2 + x + 1) = 2$.

Errores más comunes. (a) No es cierto en general que $\mathbb{Q}(\alpha + 5\alpha^2)$ sea igual a $\mathbb{Q}(\alpha)$. La inclusión $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha + 5\alpha^2)$ puede ser falsa dependiendo de α.

(c) Hay que justificar que $[\mathbb{Q}(\zeta) : \mathbb{Q}(\cos(2\pi/31))] = 2$.

Solución del problema 3. (a) **Falso.** Si fuera radical, existirían

$$L_0 = \mathbb{Q} \subset L_1 \subset \cdots \subset L_n \qquad \text{con} \qquad L_n = \mathbb{Q}(\sqrt{1 + \sqrt{\pi}})$$

y L_j/L_{j-1} algebraicas y simples, en particular finitas, pero esto es una contradicción, porque $\pi \in L_n$ con $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$, al ser π trascendente.

(b) **Falso.** Por ejemplo el ideal $I = \langle 4\rangle$ (parte real e imaginaria múltiplos de cuatro) no es maximal ya que es evidente que

$$\{0\} \subsetneq I \subsetneq \langle 2\rangle \subsetneq \mathbb{Z}[i].$$

(c) **Verdadero.** Según el teorema de clasificación de cuerpos finitos, el único cuerpo (salvo isomorfismos) de 32 elementos es $\mathbb{F}_{2^5}$, que tiene grado 5 sobre $\mathbb{F}_2 = \{0, 1\}$. Cualquier subcuerpo M debe tener grado sobre $\mathbb{F}_2$ dividiendo a 5. Si fuera 1, coincidiría con el cuerpo base $\mathbb{F}_2$ y si fuera 5 con el total.

(d) **Verdadero.** La extensión $L/\mathbb{Q}$ es de Galois. Cada elemento del grupo de Galois queda caracterizado por la permutación que induce entre las tres raíces del polinomio, por tanto $\mathcal{G}(L/\mathbb{Q})$ es isomorfo a un subgrupo de S_3. Como $|\mathcal{G}(L/\mathbb{Q}(\alpha))| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ donde α es una raíz del polinomio, se tiene que $\mathcal{G}(L/\mathbb{Q})$ tiene orden mayor que 3, de hecho múltiplo de 3. Esto reduce las posibilidades a A_3 y al propio S_3. En ambos casos hay un elemento de orden 3.

Errores más comunes. (b) El anillo $\mathbb{Z}[i]$ **no** es un cuerpo aunque sea isomorfo a $\mathbb{Z}[x]/\langle x^2+1\rangle$ y x^2+1 sea irreducible sobre $\mathbb{Z}$. Este argumento es válido cuando se trata de polinomios irreducibles sobre un cuerpo, y no sobre un anillo.

El elemento $i \in \mathbb{Z}[i]$ es una unidad, ya que $i \cdot (-i) = 1$, por lo tanto $\langle i \rangle = \mathbb{Z}[i]$; el conjunto de los números pares no es un ideal de $\mathbb{Z}[i]$; ningún $\mathbb{Z}_n$ es un ideal de $\mathbb{Z}[i]$, ni siquiera es un subconjunto de $\mathbb{Z}[i]$.

(c) El cuerpo $\mathbb{F}_{32}$ no es isomorfo al anillo $\mathbb{Z}_{32}$.

(d) Si G es el grupo de Galois de un polinomio irreducible de grado 3 sobre $\mathbb{Q}$, esto no quiere decir necesariamente que G tenga orden 3, como mucho podemos asegurar que 3 divide al orden de G.

Solución del problema 4.

El cuerpo de descomposición es $L = \mathbb{Q}(\sqrt[4]{7}, i\sqrt[4]{7}) = \mathbb{Q}(\sqrt[4]{7}, i)$.

(a) $\mathcal{L}/\mathbb{Q}$ abeliano $\Rightarrow$ todos sus subgrupos son normales $\Rightarrow$ (por el tma fundamental) todos los subcuerpos dan extensiones normales sobre $\mathbb{Q}$. Pero $\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q}$ no es normal ($x^4 - 7$ es irreducible sobre $\mathbb{Q}$ y sólo tiene dos raíces en $\mathbb{Q}(\sqrt[4]{7})$).

(b) Según el enunciado, $\sigma(\sqrt[4]{7}) = -\sqrt[4]{7}$ y $\sigma(i) = i$. Por otra parte, dividiendo (multiplicando por el inverso) las igualdades $\gamma(-i\sqrt[4]{7}) = -\sqrt[4]{7}$ y $\gamma(-i) = i$, se tiene $\gamma(\sqrt[4]{7}) = i\sqrt[4]{7}$, y por supuesto $\gamma(i) = -i$. Como $\{1, i\}$ y $\{1, \sqrt[4]{7}, \sqrt[4]{7^2}, \sqrt[4]{7^3}\}$ son bases de $L/\mathbb{Q}(\sqrt[4]{7})$ y $\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q}$, todo elemento $x \in L$ se escribe de forma única como:

$$x = \lambda_0 + \lambda_1\sqrt[4]{7} + \lambda_2\sqrt[4]{7^2} + \lambda_3\sqrt[4]{7^3} + \lambda_4 i + \lambda_5 i\sqrt[4]{7} + \lambda_6 i\sqrt[4]{7^2} + \lambda_7 i\sqrt[4]{7^3}.$$

La relación $\sigma(x) = x$ implica que todos los coeficientes de potencias impares de $\sqrt[4]{7}$ se anulan, ya que $\sigma(\sqrt[4]{7}) = -\sqrt[4]{7}$. Por tanto

$$x = \lambda_0 + \lambda_2\sqrt[4]{7^2} + \lambda_4 i + \lambda_6 i\sqrt[4]{7^2}.$$

Imponiendo ahora $\gamma(x) = x$ se tiene $\lambda_2 = \lambda_4 = 0$. De esta forma, $x \in \langle \sigma, \gamma \rangle$ si y sólo si $x = \lambda_0 + \lambda_6 i\sqrt[4]{7^2}$. En consecuencia el cuerpo fijo es $\mathbb{Q}(i\sqrt{7})$.

Errores más comunes. (a) Sólo hay dos grupos de orden 4 salvo isomorfismos: $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$, y los dos son abelianos.
